Claims:

What is claimed is:

1. In quantum cipher communication using a light signal, a quantum cipher communication system characterized by the step of detecting eavesdropping based on a change in a quantum-mechanical probability distribution defined by an amplitude and a phase in a difference signal derived from a signal light which change is produced by an eavesdropping operation.

2. A quantum cipher communication system as set forth claim 1, in said quantum cipher communication, characterized by the steps of:

splitting a light signal from a transmission source side into an intense reference signal and a weak transmission signal which is so weak that a change in its quantum mechanical state is detectable;

imparting a phase difference between said reference signal and said transmission signal while they are in a process of transmission;

superimposing in a transmission receiving side said reference signal and said transmission signal to form two output lights which are opposite in phase and producing a difference signal which is represented by a difference between said two output lights;

deriving a frequency distribution of said difference signal as a function of a fluctuation of the quantum state of said transmission signal;

based upon or in accordance with the frequency distribution of said difference signal, making privacy (secret) keys respectively at said transmission source and receiving sides

for holding in common thereby; and

directly observing the fluctuation of the quantum state of said transmission signal.

3. A quantum cipher communication system including:

a first beam splitter for splitting a light from a light source into a transmission signal and a reference signal;

a phase modulating means for imparting a phase modulation to said transmission signal;

a light attenuator for converting said transmission signal into a weak transmission signal which is so weak that a change in its quantum state is detectable; and

a phase modulating means for imparting a phase modulation to said reference signal, said system also including, operative after a relative phase difference is imparted between said transmission and reference signals:

a second beam splitter for superimposing said phase-modulated weak transmission signal and said phase modulated intense reference signal to form two output lights;

a first and a second photoelectric conversion elements for converting said two output lights from said second beam splitter into two corresponding electric signals which are opposite in phase; and

an amplifier for amplifying a difference signal representative of a difference between said two output lights to output an amplified corresponding voltage.

4. A quantum cipher communication system as set forth in claim 3, characterized in that said phase modulating means includes a mirror movable by a distance as small as the wave length of an incident light.

5. A quantum cipher communication system as set forth in any one of claims 1 to 4, characterized in that said reference signal and said transmission signal are split both in time and as polarized and then transmitted to travel along a common path.

6. A quantum cipher communication system including:

a first beam splitter for splitting a light from a light source into a transmission signal and a reference signal;

a first light polarizer for polarizing said transmission signal through longer one of two distance paths;

a light attenuator for converting said transmission signal into a weak transmission signal which is so weak that a change in its quantum state is detectable;

a first phase modulating means for imparting a predetermined phase modulation to said transmission signal; and

a first polarized beam splitter for receiving said intense reference signal having passed through shorter one of two distance paths and said transmission signal and returning the received signal to travel along a common optical path, said system also including, operative after a relative phase difference is imparted between said transmission and reference signals and included in a transmission receiving side:

a second polarized beam splitter for isolating from each other said transmission and reference signals transmitted through a single optical fiber;

a second phase modulating means for imparting a phase modulation to said isolated transmission signal through shorter one of two distance paths; and

a second light polarizer for polarizing said isolated reference signal through longer one of two distance paths, said system further including:

a second beam splitter for superimposing said transmission and reference signals which are coincident with each other in time and polarization to produce two output lights;

a first and a second photoelectric conversion elements for converting said two output lights into corresponding electric signals which are opposite in phase; and

an amplifier for amplifying a difference signal representative of a difference between said two output lights to output an amplified corresponding voltage.

7. A quantum cipher communication system as set forth in claim 6, characterized in that a third light polarizer is provided in an output side of said optical fiber for making a correction for a disturbance of polarization of said reference signal.

8. A quantum cipher communication system as set forth in any one of claims 1 to 7, characterized in that threshold values are established, respectively, for positive and negative values of said difference signal, and that the state of said transmission signal is discriminated on the basis of said threshold values.

9. A quantum cipher communication system as set forth in any one of claims 1 to 8, characterized in that in addition to the phase modulations designed to transmit privacy keys, such a phase modulation is so imparted as described and having a value later determined for making a correction for a fluctuation of the difference in optical path between said reference signal and said transmission signal which develops by reason of an external cause.

10. A quantum cipher communication system as set forth

in any one of claims 1 to 9, characterized in that such phase modulations are so imparted as described and including those for transmitting privacy keys and those with values later determined are randomly repeated.

11. A quantum cipher communication system as set forth in any one of claims 1 to 10, characterized in that eavesdropping is detected on the basis of an increase in the error rate of said difference signal.

12. A quantum cipher communication system as set forth in any one of claims 1 to 11, characterized in that eavesdropping is detected on the basis of a change in a Wigner distribution function that indicates a quantum mechanical state of said difference signal.

13. A quantum cipher communication system as set forth in any one of claims 1 to 12, characterized in that said two output lights are converted into corresponding electric signals through photoconductor diodes.

14. A quantum cipher communication system as set forth in any one of claims 1 to 13, characterized in that for said photoconductor diodes, use is made of silicon photoconductor diodes when the light has a wave length of 600 nm to 900 nm, and of InGaAs photoconductor diodes when the light has a wave length of 1000 nm to 1500 nm.